REMARKS

Applicants appreciate the thorough examination of the present application that is evidenced in the Final Official Action of March 23, 2006 (the "Official Action").

Status of the Claims

Claims 1-5, 7, 8, 10, 11, 14, 17 and 18 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,029,206 to Marino, et al. ("Marino"). Claims 2-8, 10, 11 and 14 were rejected under 35 U.S.C § 103(a) as unpatentable over Marino in view of U.S. Patent No. 6,131,163 to Wiegel. Claims 9 and 13 were rejected under 35 U.S.C § 103(a) as unpatentable over Marino in view of U.S. Patent No. 5,845,068 to Winiger ("Winiger"). Claim 12 was rejected under 35 U.S.C § 103(a) as unpatentable over Marino in view of User Manual mod_ssl version 2.6 ("Mod_SSL"). Claim 15 was rejected under 35 U.S.C § 103(a) as unpatentable over Marino in view of U.S. Pre-Grant Publication No. 2002/0116605 to Berg ("Berg"). Claim 16 was rejected under 35 U.S.C § 103(a) as unpatentable over Wiegel in view of T. Dierks et al, "Network Working Group Request For Comments 2246, The TLS Protocol" ("Dierks").

The Claims Are Patentable Over Marino

The Official Action indicated that Claims 1-5, 7, 8, 10, 11, 14, 17 and 18 were rejected under 35 U.S.C. § 102(b) as being anticipated by Marino. Official Action, p. 2. However, in connection with the rejection under 35 U.S.C. § 102(b), the Official Action only discussed Claims 1, 17 and 18. The Examiner is requested to clarify if Claims 2-5, 7, 8, 10, 11, and 14 are rejected under 35 U.S.C. § 102(b) as being anticipated by Marino, and if so, to point out the relevant portions of Marino that disclose each and every recitation of each of those claims.

Claim 1, as amended, recites as follows (emphasis added):

> 1. (Currently Amended) A method of improving security processing in a computing network, comprising:
>
> providing security processing in an operating system kernel;
>
> providing an application program which makes use of the operating system kernel during execution;
>
> providing security policy information that is usable for more than one executing application program;

executing the application program; and

selectably encrypting at least one communication of the executing application program using the provided security processing in the operating system kernel, under conditions specified by the security policy information.

Claim 1 has been amended to include the recitations of cancelled Claim 3, namely, to clarify that the security policy information is usable for more than one executing application program. Accordingly, the patentability of amended Claim 1 will be addressed with reference to the rejection of Claims 1 and 3.

As explained in the specification, security policy information may be used to provide conditions for security processing, according to some embodiments of the invention. See App., p. 15, l. 11 to p. 17, l. 9. According to embodiments of the invention, security policy information may be established by an administrator, and may be used to enable security processing for particular ports, jobs, clients, source/destination addresses, etc., App., p. 15, l. 7 to p. 16, l. 13. Such security policy information may be available to the kernel when an application program seeks to establish a communication session, and need not be provided by, or even known to, the application program. Thus, SSL enablement may be performed by the stack, "removing the need for the application to negotiate SSL." App., p. 16, ll. 10-11. Accordingly, the use of security policy information provides a system administrator with "fine grained control for both server and client applications." App., p. 16, ll. 7-8. Such control may be exercised by a system administrator to provide a consistent policy for all applications. App., p. 15, l. 7 to p. 16, l. 6. In addition, such control may be used to provide security processing for application programs that are not aware that security processing is taking place, i.e., so called non-SSL applications. App., p. 16, l. 17 to p. 17, l. 1.

In sharp contrast to the present invention, the system of Marino relies on information provided to the security processing modules by the application programs themselves. As stated in Marino:

> An application program of the red processing side initiates a request to the KMUA as depicted by transfer 101. The application software passes along to the KMUA 40 a number of parameters. These parameters include the title or name of the remote subsystem with which the cryptographic association is to be established. Next, the red

> side application software indicates via a parameter what cryptographic algorithm is to be selected for the data encryption and decryption. Further parameters passed by the application software to KMUA 40 include options and crypto modes. These modes indicate such parameters as one-way or two-way traffic encryption keys or other considerations related to a specific algorithm to be used.

Marino, col. 7, ll. 36-50. Accordingly, in the system of Marino, when a secure communication session is to be established, security information is passed from the application program to the security kernel. This is in direct contrast to systems and methods of the present invention, in which security policy information is provided in an operating system kernel, for example by an administrator, and may be used to selectively encrypt a communication of more than one executing application program, as recited in Claim 1.

As explained above, in some embodiments of the invention, the application program need not be aware that security processing exists. In contrast, an application program running under the system of Marino must have explicit awareness of the security kernel in order to invoke its functions by means of a request to the KMUA.

Accordingly, Marino does not teach or suggest many of the recitations of Claim 1, and Applicant respectfully requests that the rejection of Claim 1 as anticipated by Marino be withdrawn.

The Claims are Patentable Over Marino and Wiegel

As explained in the previous Amendment, Wiegel discloses a system for a network gateway that provides computer data security using a protocol stack proxy. See Wiegel, Abstract. In particular, Wiegel describes a system for detecting whether requests to a system are accurate, valid and come from an authorized system. Weigel, col. 1, ll. 47-50. That is, Wiegel is concerned with repelling unauthorized requests and malicious attacks originating outside a computer system. *See* Wiegel, col. 1, ll. 51-55.

Applicants respectfully submit that Wiegel and Marino cannot be properly combined. The Official Action states that it would have been obvious to modify the system of Marino to include the system of Wiegel "because Wiegel offers increased assurance that communications coming into and out of individual computers over a network are authentic which would improve upon Marino's invention of increasing securing of communications amongst computers at the kernel level within a network." Official Action at 5. Thus, the Official Action appears to be stating that there is motivation to combine the references because the combined system would have the functionality of both Marino and Wiegel. Applicants respectfully submit that the test for combining references is not whether the combination would provide additional functionality, because that is always the case with an aggregation such as the one hypothesized in the Official Action. Rather, the appropriate test is whether there is a motivation, found explicitly or implicitly within the references, to combine them to produce the claimed invention. Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art. "The test for an implicit showing is what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art." In re Kotzab, 217 F.3d 1365, 1370, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000)

In this case, a skilled person would not be motivated to combine a reference that teaches a system for managing port-level system requests (Wiegel) with a reference related to the encryption of data in a communications system (Marino) absent some express teaching in the references. As no such teaching has been identified in the Official Action, a prima facie showing of obviousness has not been made. Furthermore, a skilled person would not be motivated to modify the system of Marino as suggested in the Official Action, since, as explained above, in the system of Marino, security processing is performed based on information provided by the application program. As stated in Marino, "[w]hen the black or red application software or processes call the security kernel 6 for various functions, it is accomplished via the passage of parameters from the application processes to the security kernel. Each function supported by the security kernel **requires different parameters** and performs a different security function." Marino, col. 7, ll. 18-25 (emphasis added). Given that the security functions of Marino require different parameters that are supplied by the applications themselves, it is not clear how, if the policy tree of Wiegel were combined with the system of Marino, the system of Marino would be able to provide security processing to the application processes.

Moreover, even if combined, Wiegel and Marino do not teach the claimed invention, since the policy tree of Wiegel is not used to encrypt a communication of an executing application program, but rather is simply used to define acceptable protocols for a given port. See Wiegel, col. 9, ll. 23-41.

Accordingly, Applicants submit that Claim 1 is patentable over the Marino in view of Wiegel.

Claims 17 and 18 contain similar recitations as Claim 1, and are submitted to be allowable for the reasons explained above with respect to Claim 1. Dependent Claims 2 and 4-16 are patentable at least as per the patentability of Claim 1.

CONCLUSION

In light of the above amendments and remarks, Applicants respectfully submit that the above-entitled application is in condition for allowance. Favorable reconsideration of this application is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,

David C. Hall
Registration No. 38,904

Customer Number 46589
Myers Bigel Sibley & Sajovec, P.A.
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
919-854-1401 (Fax)